Appendix 7: Public Disclosure Exemptions

Critical infrastructure information may find exemption from public disclosure under one of the following subsection exemptions, applicable to critical infrastructure protection, as specified in Revised Code of Washington (RCW) 42.17.310:

310(h) Valuable formulae, designs, drawings, computer source code or object code, and research data obtained by any agency within five years of the request for disclosure when disclosure would produce private gain and public loss.

310(i) Preliminary drafts, notes, recommendations, and intra-agency memorandums in which opinions are expressed or policies formulated or recommended except that a specific record shall not be exempt when publicly cited by an agency in connection with any agency action.

310(ww) Those portions of records assembled, prepared, or maintained to prevent, mitigate, or respond to criminal terrorist acts, which are acts that significantly disrupt the conduct of government or of the general civilian population of the State or the United States and that manifest an extreme indifference to human life, the public disclosure of which would have a substantial likelihood of threatening public safety, consisting of:

(i) Specific and unique vulnerability assessments or specific and unique response or deployment plans, including compiled underlying data collected in preparation of or essential to the assessments, or to the response or deployment plans; and

(ii) Records not subject to public disclosure under Federal law that are shared by Federal or international agencies, and information prepared from national security briefings provided to State or local government officials related to domestic preparedness for acts of terrorism.

{Note: Under Federal law, the exemptions to the Freedom of Information Act, under 5 U.S.C. §552(b) that may apply to critical infrastructure information, which the State of Washington accepts and adheres include:

552(b)(1)(A) [Information] specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order.

552(b)(3) [Information] specifically exempted from disclosure by statute (other than Section 552b of this title), provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;

552(b)(4) Trade secrets and commercial or financial information obtained from a person and privileged or confidential;

552(b)(7) Records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information

(A) could reasonably be expected to interfere with enforcement proceedings,

(D) could reasonably be expected to disclose the identity of a confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of a record or information compiled by criminal law enforcement authority in the course of a criminal investigation or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source,

(E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or

(F) could reasonably be expected to endanger the life or physical safety of any individual.}

310(ccc) Information compiled by school districts or schools in the development of their comprehensive safe school plans pursuant to RCW 28A.320.125, to the extent that they identify specific vulnerabilities of school districts and each individual school.

310(ddd) Information regarding the infrastructure and security of computer and telecommunications networks, consisting of security passwords, security access codes and programs, access codes for secure software applications, security and service recovery plans, security risk assessments, and security test results to the extent that they identify specific system vulnerabilities.